Amendments to the Claims:

The following listing of the claims replaces all previous listings and versions of the claims in the application:

Listing of the Claims:

Claims 1-19: (Cancelled)

20. (New) A method of establishing a communication path from a first identity device in a data communication network, comprising the steps of:

      providing a one-time-only private reference point in said data communication network;

      establishing a communication path from the first identity device to said one-time-only private reference point;

      verifying the authentication of the first identity device relative to said one-time-only private reference point from said first identity device; and

      establishing communication from said one-time-only private reference point to a second identity device through said data communication network;

      wherein at least one of the steps of verifying the authentication and establishing communication is performed without disclosing the identity of said first identity device.

21. (New) The method according to claim 20, further comprising the preliminary steps of:

      authenticating said first identity device by registering data selected from the group consisting of biometrics, a signature, a code and any combinations thereof; and

      comparing the registered data with correspondingly stored data.

22. (New) The method of claim 20, wherein the step of verifying is performed without disclosing the identity of the first identity device.

23. (New) The method of claim 20, wherein the step of establishing communication is performed without disclosing the identity of the first identity device.

24. (New) The method according to either of claims 20 or 21, wherein said first identity device comprises a card including encrypted data, said method further comprising:

said first identity device receiving an encrypted key from said one-time-only private reference point;

decrypting said encrypted key using a second stored key; and

decrypting said encrypted data using said key.

25. (New) The method according to either of claims 20 or 21, said communication network being selected from the group consisting of a personal area network, local area network, a wide area network, a global area network, the Internet, a radio network, a public switched telephone network (PSTN), a global system for mobile communications (GSM) network, a code division multiplex access (CDMA) network, a universal mobile telecommunications system (UMTS) network, and any combinations thereof.

26. (New) The method according to either of claims 20 or 21, said first identity device having an authenticated holder, and said one-time-only private reference point being addressable by the authenticated holder from a computer communicating with said data communication network.

27. (New) The method according to either of claims 20 or 21, further comprising said first identity device allowing or blocking access to said one-time-only private reference point by a third identity device.

28. (New) The method according to claim 27, wherein said third identity device is a party selected from the group consisting of a third party and said first identity device.

29. (New) The method according to either of claims 20 or 21, wherein said step of establishing communication involves creating and negotiating an accountability path dynamically adapted to a context risk profile.

30. (New) The method according to claim 29, wherein said first identity device has an authenticated holder, and said second identity device establishes a procedure to identify a party selected from the group consisting of said first identity device and the authenticated holder of said first identity device.

31. (New) The method according to claim 30, wherein said procedure to identify a party employs identification information selected from the group consisting of at least one of biometrics, name, digital signature, and a code.

32. (New) The method according to either of claims 20 or 21, further comprising:

    providing an identity provider and a service provider;

    establishing communication from said second identity device to said service provider;

    establishing communication from said service provider to said identity provider;

    providing a further identity device corresponding to a financial institution;

    establishing communication from said service provider to said further identity device;

    transmitting information from said second identity device to said service provider;

    transmitting said information from said service provider to said identity provider;

    transmitting said information from said identity provider to said further identity device;

    said further identity device responding to said information by transmitting a payment acceptance to said identity provider;

    said identity provider transmitting payment accept to said service provider; and

    said service provider transmitting payment accept to said second identity device.

33. (New) A system for establishing a communication path from a first identity device in a data communication network, comprising:

    a one-time-only private reference point in said data communication network; and

    a first communication path defined from said first identity device to said one-time-only private reference point;

    means for verifying the authentication of said first identity device relative to said one-time-only private reference point from said first identity device; and

means for establishing a second path of communication from said one-time-only private reference point to a second identity device through said data communication network;

wherein at least one of the means for verifying the authentication and the means for establishing communication is operable without disclosing the identity of said first identity device to said second identity device.

34. (New) The system according to claim 33, wherein said one-time-only private reference point is stored on a server communicating with said data communication network.

35. (New) The system according to either of claims 33 or 34, wherein said data communication network is selected from the group consisting of a personal area network. local area network. a wide area network, a global area network, the Internet, a radio network, a public switched telephone network (PSTN), a global system for mobile communications (GSM) network, a code division multiplex access (CDMA) network, a universal mobile telecommunications system (UMTS) network, and any combinations thereof.

36. (New) The system according to either of claims 33 or 34, wherein said first identity device comprises a card including encrypted data for verifying the authentication of the first identity device relative to said one-time-only said private reference point.

37. (New) The system according to either of claims 33 or 34, wherein said means for verifying employs data selected from the group consisting of at least one of biometrics. and codes, and digital signatures.

38. (New) The system according to either of claims 33 or 34, wherein said means for verifying the authentication is operable without disclosing the identity of said first identity device to said second identity device.

39. (New) The system according to either of claims 33 or 34, wherein said means for establishing communication is operable without disclosing the identity of said first identity device to said second identity device.